حمله XSS چیست؟

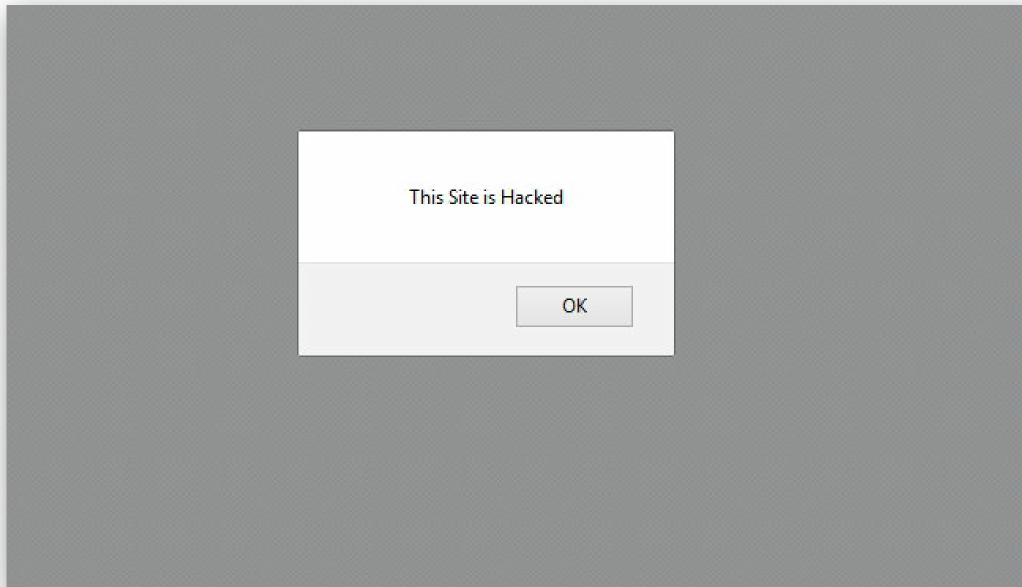
XSS مخفف عبارت **Cross-Site-Scripting** است و به دلیل اینکه با CSS اشتباه گرفته نشود ابتدای آن را با حرف X شروع می کنند.
در این نوع حمله نفوذگر **اسکریپتهای جاوااسکریپت** یا **برچسب های HTML** دلخواه خود را به صفحه قربانی **تزریق** کرده و این **کدهای مخرب** روی مرورگر کاربران دیگر سایت اجرا میشود.

فرض کنید یک سایت نظر سنجی که کاربران نظرات خود را درج می کنند و نظرات دیگران را نیز مشاهده می کنند، در برابر **حمله XSS** آسیب پذیر باشد.
خب دراینجا شخص نفوذگر **کد جاوااسکریپت** زیر را در قسمت ثبت نظر وارد می کند:

```
<script>alert("This Site is Hacked");</script>
```

comment: <script>alert("This Site is Hacked");</script> Submit

از آنجایی که برای مقابله با **حملات XSS** تدابیری انجام نشده پس کد بالا در صفحه ذخیره و توسط مرورگر چاپ و سپس اجرا می شود که حاصل کار نمایش متن اخطار به تمامی کاربران است:



اگر نگاهی به source صفحه پس از حمله بیندازیم متوجه می شویم که کد عینا در صفحه چاپ شده است که همین موجب اجرای آن در صفحه توسط مرورگر شده است:

```
<script>alert("This Site is Hacked");</script>
```

قطعا برای شما اکنون این سوال پیش آمده که یک کد هشدار در صفحه نمی تواند اطلاعات کاربران را به سرقت ببرد. قطعا درست است. اما شخص نفوذگر توسط کد زیر می تواند به کوکی های تمامی کاربران دسترسی داشته باشد:

```
&lt;script&gt;alert(&quot;This Site is Hacked&quot;);&lt;/script&gt;gt;
```

جلوگیری از حمله xss

بهترین روش برای جلوگیری از **حمله xss در php** این است که شما **کاراکترهای خاص** که اغلب در کدهای جاوااسکریپت مورد استفاده قرار می گیرند را به شکل **معادل آن در html** بنویسیم تا از اجرای آن توسط مرورگر جلوگیری کنیم.

بعض از این کارکترها و معادل آنها در HTML به شرح زیر است:

نمونه هایی از کاراکترهای خاص و معادل آنها در HTML

Special Character	Character
&lt	<
&gt	>
&amp	&
&quot	“
&#64	@

روش جلوگیری از حمله xss در php

اما در php چگونه کاراکترهای خاص را به معادل آنها در HTML تبدیل کنیم؟

جواب استفاده از تابع ()htmlspecialchars در php می باشد. این تابع کاراکتر های خاص را در ورودی هایی که کاربران ارسال کرده اند شناسایی می کند و آن ها را به معادل آن در HTML تبدیل می کند. می توانید ورودی هایی که توسط کاربران به سایت شما ارسال می شوند را توسط این تابع فیلتر کنید:

```
htmlspecialchars($_GET['comment']);
```

کد جاوا اسکریپت بالا پس از ارسال به این تابع به شکل زیر تبدیل می شود و از اجرای آن جلوگیری می شود:

```
&lt;script&gt;alert(&quot;This Site is Hacked&quot;);&lt;/script&gt;
```